

REMARKS

Claims 1-4, 6, 7, 9-17 and 19-26 are pending, of which claims 1, 19, and 22 are independent method claims with independent computer program product claim 12 corresponding to independent method claim 1. As indicated above, no claims have been amended by this response.

The Office Action rejected all of the independent claims 1, 12, 19, and 22 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,324,648 issued to Grantges, Jr. (the patent hereinafter referred to as "Grantges"). The remaining dependent claims were rejected as either anticipated under 35 U.S.C. § 102(e) by Grantges or as unpatentable under 35 U.S.C. § 103(a) over Grantges in view "Wireless Application Protocol Wireless Transport Layer Security" by En (the reference hereinafter referred to as "En").

Accompanying this response is an affidavit under 37 C.F.R. 1.131 swearing behind Grantges by establishing a date of invention on, at the latest, December 13, 1999, which pre-dates the provisional priority filing date of Grantges. Accordingly, Grantges no longer qualifies as prior art under 35 U.S.C. 102(e), and thus all of the rejections should be withdrawn.

However, even without the 37 C.F.R. 1.131 affidavit, the undersigned respectfully submits that Grantges does not anticipate any of the independent claims. For instance, Applicants' invention, as claimed for example in independent method claim 1, relates to a communications device of an external client establishing a secure connection over a public network to a private network without restricting the communications device to working through the private network. The method includes the external client establishing a connection with a virtual private network access server of the private network over the public network using the communication device, the virtual private network server providing the external client access to the private network as though the external client is part of the private network; providing security to the connection through a communication protocol that resides at or above a socket layer in a protocol stack the external client uses to communicate data; maintaining a session that uses the secure connection to communicate with the private network; and during at least a portion of maintaining a session that uses the secure connection, the communication device retaining the ability to establish a separate and distinct connection with another resource outside

of the private network. Independent claim 12 recites similar limitations from the perspective of a computer program product.

Applicants' invention, as claimed for example in independent method claim 19, similarly relates to a communications device of an external client establishing a secure connection over a public network to a private network without restricting the communications device to working through the private network. The method includes securely connecting to a virtual private network access server of the private network through a communication protocol that resides at or above a socket layer in a protocol stack that the external client uses to communicate data in order to retain the ability to establish a separate and distinct connection with a resource outside of the private network, the virtual private network access server providing the external client access to the private network as though the external client is part of the private network; and while securely connected to the virtual private network access server, a specific act of accessing the resource outside of the private network.

Applicants' invention, as claimed for example in independent method claim 22, relates to a server computer system within a private network establishing a secure connection with a communications device of an external client without restricting the communications device to working through the private network. The method includes a virtual private network access server within the private network facilitating the establishment of a connection with the external client over the public network, the virtual private network server providing the external client access to the private network as though the external client is part of the private network; and facilitating the providing of security to the connection through a communication protocol that resides at or above a socket layer in a protocol stack used to communicate data, wherein the secure connection is established while allowing the external client to maintain the ability to establish a separate and distinct connection directly with one or more external resources rather than having to route communication with the one or more external resources through the private network.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131. That is, "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly." MPEP § 706.02. Applicants also note that "[i]n determining that quantum of prior art disclosure which is necessary to declare an applicant's

invention 'not novel' or 'anticipated' within section 102, the stated test is whether a reference contains an 'enabling disclosure.'" MPEP § 2121.01. In other words, a cited reference must be enabled with respect to each claim limitation. During examination, the pending claims are given their broadest reasonable interpretation, *i.e.*, they are interpreted as broadly as their terms reasonably allow, consistent with the specification. MPEP §§ 2111 & 2111.01.

Grantges discloses a network system that is configured to provide access by a user of an external client to one of a number of software applications within a private network. Since the communication with the private network is exclusively using HTTP or HTTPS, each software application has an associated web server. However, if the client were part of the network, they would not be limited to HTTP or HTTPS communications. In contrast, Claim 1 recites "establishing a connection with a virtual private network access server of the private network over the public network using the communication device, the virtual private network server providing the external client access to the private network as though the external client is part of the private network". A VPN server such as the recited "virtual private network access server" supports a wide variety of communication methodology. Thus, the use of a VPN server does allow the external client to experience the network as though the external client was part of the private network. Grantges does not teach or suggest the use of such a VPN server. Thus, Claim 1 is not anticipated by Grantges. For similar reasons, the remaining independent claims are also not anticipated by Grantges.

Based on at least the foregoing reasons, therefore, Applicants respectfully submit that the cited prior art fails to anticipate or make obvious Applicants invention, as claimed for example, in independent claims 1, 12, 19, and 22, regardless of whether or not the 37 C.F.R. 1.131 affidavit is accepted. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertion with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable, and Applicants reserve the right to do so.

In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 28th day of October, 2005

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
ADRIAN J. LEE
Registration No. 42,785
Attorney for Applicant
Customer No. 47973